AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A 2016 TESLA MODEL X, VIN 5YJXCDE45GF026419.

Case No. 2:21-mj-513

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

1409 Bonita Avenue, Las Vegas, Nevada, including all adjacent parking areas and/or garages and/or outbuildings associated with those locations.

located in the _____ District of Nevada, there is now concealed *(identify the person or describe the property to be seized)*:

A 2016 Tesla Model X, VIN 5YJXCDE45GF026419, including all keys for said vehicle and any and all ownership and registration documents.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☐ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841 et seq. and/or § 846 and/or 18 U.S.C. § 1956	Controlled Substances Violations and/or Money Laundering

The application is based on these facts:
See attached affidavit incorporated by reference herein.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Stephen Blunk
Applicant's signature

Stephen Blunk, IRS-CI Special Agent
Printed name and title

Sworn to before me and signed in my presence. VIA FaceTime

Date: 8/2/2021

Judge's signature

City and state: Columbus, OH

Elizabeth Preston Deavers, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEARCH AND SEIZURE WARRANTS

I, Stephen Blunk, being duly sworn under oath, depose and say:

INTRODUCTION

1. I am a Special Agent with the United States Department of Treasury, Internal Revenue Service, Criminal Investigations (IRS-CI). I have been employed as an IRS-CI Special Agent since August 1998 and am presently assigned to the Cincinnati Field Office, Columbus, Ohio, post of duty. During my employment with IRS-CI, I have investigated violations of the Internal Revenue laws and related offenses, including but not limited to money laundering. As an IRS-CI Special Agent, I have investigated or been involved in investigations related to violations of offenses under Titles 18, 21, 26, and 31 of the United States Code.

2. During the course of my employment as an IRS-CI Special Agent, I have provided financial investigative expertise and assistance to the Drug Enforcement Administration (DEA), Homeland Security Investigations (HSI), and various other federal and local law enforcement agencies, related to investigations of individuals and organizations involved in criminal activity to include those who derive substantial income from the importation, manufacture, distribution, and sale of illegal controlled substances. I am currently assigned to the South-Central High Intensity Drug Trafficking Area Cyber Taskforce (SCHCTF) in Columbus, Ohio, where my involvement includes the documentation and transactional analysis of illegal proceeds obtained in violation of various federal and state statutes, to include the laundering of proceeds derived from trafficking in controlled substances via dark web marketplaces.

3. I have experience in the execution of narcotics and financial documentary search warrants, and the debriefing of defendants, witnesses, informants and other persons who have knowledge of the amassing, spending, converting, transporting, distributing, laundering and concealing of the proceeds of narcotic and other illegal activities. I have experience in investigating financial crimes committed by individuals who traffic in illegal controlled substances and thus commit violations of offenses under Titles 18, 21, 26, and 31 of the United States Code.

4. I have participated in the execution of search and seizure warrants. These warrants have included the search of businesses and residences of individuals involved with the laundering of illegally derived proceeds and individuals who have evaded income taxes. These warrants have also included the seizure of proceeds derived from a specified unlawful activity (SUA) or illegally derived proceeds that have been deposited into financial-related accounts, or used to purchase assets, etc.

5. This affidavit is based upon my personal knowledge, information from witnesses and other law enforcement personnel, my review of documents and other evidence, my conversations with other law enforcement personnel, both domestic and foreign, and my personal training and experience as a criminal investigator. Because it is submitted for the limited purpose of establishing probable cause for a seizure warrant, this affidavit does not necessarily recite all of the facts that are known to me or to other law enforcement at this time. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

6. Based on my training, experience, and participation in drug trafficking and dark web investigations, I know and have observed the following:

a. I have learned about the manner in which individuals and organizations distribute controlled substances throughout the United States;

b. I know drug traffickers often purchase and/or title assets in fictitious names, aliases or the names of relatives, associates, or business entities to avoid detection of these assets by government agencies. I know that even though these assets are in the names other than the drug traffickers, the drug traffickers actually own and continue to use these assets and exercise dominion and control over them;

c. I know drug traffickers must maintain on-hand large amounts of crypto-currency and U.S. currency to include stored in financial accounts and/or wallets which are readily accessible in order to maintain and finance their ongoing drug business;

d. I know when drug traffickers amass large proceeds from the sale of drugs, the drug traffickers attempt to legitimize these profits through money laundering activities. To accomplish these goals, drug traffickers utilize the following methods, including, but not limited to: domestic and international banks and their attendant services, crypto-currency exchanges, peer-to-peer services, securities brokers, professionals such as attorneys and accountants, casinos, real estate, shell corporations and business fronts and otherwise legitimate businesses which generate large quantities of currency; and

e. I know that Bitcoin and other crypto currency accounts are often times used by drug traffickers to launder money or conceal drug proceeds because of the

anonymity associated with the use of Bitcoin and other crypto currency accounts and because crypto currency is decentralized.

PURPOSE OF AFFIDAVIT

7. This affidavit is submitted in support of an application for seizure warrants for the following:

a. A 2016 Tesla, Model X, a passenger vehicle, with a Vehicle Identification Number (VIN) 5YJXCDE45GF026419, including all keys and any and all ownership and/or registration documents for said vehicle; and

b. All funds and/or digital currencies in Wealthfront Brokerage account #8W285396 (hereinafter referred to as WFB#5396), in the name of James BARLOW.

(collectively, hereafter, the "SUBJECT ASSETS"). This affidavit is also submitted in support of an application for a search warrant for the limited purpose of seizing the 2016 Tesla from the residence located at 1409 Bonita Avenue, Las Vegas, Nevada, 89104.

8. As set forth below, I submit that there is probable cause to believe that the SUBJECT ASSETS are property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of violations of 21 U.S.C. § 841 (To manufacture, distribute, or dispense a controlled substance) and 21 U.S.C. § 846 (conspiracy to distribute and possess with intent to distribute, controlled substances, including distribution by means of the Internet). The SUBJECT ASSETS are therefore subject to forfeiture to the United States under 21 U.S.C. § 881(a) (civil forfeiture) and/or 21 U.S.C. § 853(a) (criminal forfeiture).

9. I further submit that there is probable cause to believe that the SUBJECT ASSETS constitute property involved in a money laundering transaction or money

laundering conspiracy, in violation of 18 U.S.C. § 1956, or are traceable to such property. The SUBJECT ACCOUNT is, therefore, subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1) (civil forfeiture) and/or 982(a)(1) (criminal forfeiture).

10. Because this affidavit is submitted for the limited purpose of obtaining warrants authorizing the search and seizure of the SUBJECT ASSETS, I am not including every fact known to me about the DEFENDANT or the larger investigation.

11. This affidavit is based upon my own personal observations, my training and experience, discussions with other agents who are familiar with this investigation, and information collected during this investigation through, among other things, witness interviews, law enforcement investigation reports, information obtained through searches, and public records.

FORFEITURE AND SEIZURE AUTHORITY

12. As to civil forfeiture, under 21 U.S.C. § 881(a), "[t]he following shall be subject to forfeiture to the United States and no property right shall exist in them: . . . (6) All moneys, negotiable instruments, securities, or other things of value furnished or intended to be furnished by any person in exchange for a controlled substance or listed chemical in violation of this subchapter, all proceeds traceable to such an exchange, and all moneys, negotiable instruments, and securities used or intended to be used to facilitate any violation of this subchapter." Property subject to civil forfeiture under 21 U.S.C. § 881(a) may be seized pursuant to 18 U.S.C. § 981(b) (by 21 U.S.C. § 881(b)).

13. Pursuant to 18 U.S.C. § 981(a)(1)(A), "[a]ny property, real or personal, involved in a transaction in violation of [18 U.S.C. §§ 1956], or any property traceable to such

property" is subject to forfeiture to the United States. Property subject to civil forfeiture under 18 U.S.C. § 981(a)(1) may be seized pursuant to 18 U.S.C. § 981(b).

14. As to criminal forfeiture, under 21 U.S.C. § 853(a), "[a]ny person convicted of a violation of this subchapter or subchapter II of this chapter punishable by imprisonment for more than one year shall forfeit to the United States, irrespective of any provision of State law [*inter alia*]—(1) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; [and] (2) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation." As property subject to criminal forfeiture under 21 U.S.C. § 853(a), the SUBJECT ASSETS may be seized pursuant to 21 U.S.C. § 853(f). Under 21 U.S.C. § 970, Section 853 applies in every respect to a violation of this subchapter punishable by imprisonment for more than one year, including violations of 21 U.S.C. § 963.

15. Under 18 U.S.C. § 982(a)(1), "[t]he court, in imposing sentence on a person convicted of an offense in violation of 18 U.S.C. §§ 1956 shall order that the person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property." As property subject to criminal forfeiture under 18 U.S.C. § 982(a)(1), the SUBJECT ASSETS may be seized pursuant to 21 U.S.C. § 853(f) (by 18 U.S.C. § 982(b)(1).

16. With respect to seizure, 21 U.S.C. § 853(f) specifically provides that a court may issue a criminal seizure warrant when it "determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that a[] [protective] order under [21 U.S.C. § 853(e)] may not be sufficient to assure the availability of the property for forfeiture." As set forth further below, there is a substantial

risk that the SUBJECT ASSETS will be withdrawn, moved, dissipated, or otherwise become unavailable for forfeiture unless immediate steps are taken to secure them. I therefore submit that a protective order under 21 U.S.C. § 853(e) would not be sufficient to assure that the SUBJECT ASSETS will remain available for forfeiture.

17. Furthermore, pursuant to 18 U.S.C. § 981(b)(3), "[n]otwithstanding the provisions of rule 41(a) of the Federal Rules of Criminal Procedure, a seizure warrant may be issued pursuant to this subsection by a judicial officer in any district in which a forfeiture action against the property may be filed under section 1355(b) of title 28, and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement."

18. For the reasons listed above, the United States seeks a combined criminal and civil seizure warrant, authorizing law enforcement to seize the SUBJECT ASSETS and preserve it pending further forfeiture proceedings.

BACKGROUND ON THE DARK WEB & CRYPTOCURRENCY

19. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. The "dark web" is a portion of the "deep web[1]" of the Internet, where individuals must use an anonymizing software or application called a "darknet" to access content and websites. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes

[1] The deep web is the portion of the Internet not indexed by search engines. Examples are databases and internal networks belonging to private industry, government agencies, or academic institutions.

called the "clear web" or simply the "web"). These online market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring. Famous dark web marketplaces ("DWM's"), also called Hidden Services, such as Silk Road 1, Silk Road 2, AlphaBay, and Hansa (all of which have since been shut down by law enforcement), operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services. When law enforcement shut down the four DWM's listed above, they also obtained images of their servers, and law enforcement has been able to mine the data from those sites for information about the customers and vendors who used them.

b. "Vendors" are the dark web's sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of "vendor accounts" on dark web marketplaces. Customers, meanwhile, operate "customer accounts." Vendor and customer accounts are not identified by numbers, but rather monikers or "handles," much like the username one would use on a clear web site. If a moniker on a particular marketplace has not already been registered by another user, vendors and customers can use the same moniker across multiple marketplaces, and based on seller and customer reviews, can become well known as "trusted" vendors or customers. It is also possible for the same person to operate multiple customer accounts and multiple vendor accounts at the same time. For example, based on my training and experience, I know that one person could have a vendor account that he or she uses to sell illegal goods on a dark web marketplace in exchange for cryptocurrency; that same vendor could also have a different customer account that he or she uses to exchange cryptocurrency earned from vendor

sales for fiat currency[2]. Because they are separate accounts, a person could use different accounts to send and receive the same cryptocurrency on the dark web. I know from training and experience that one of the reasons dark web vendors have multiple monikers for different vendor and customer accounts, is to prevent law enforcement from identifying which accounts belong to the same person, and who the actual person is that owns or uses the accounts.

c. The "Tor network," or simply "Tor" (an abbreviation for "The Onion Router"), is a special network of computers on the Internet, distributed around the world, designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor also enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such hidden services operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software, including a browser known as "Tor Browser," designed to access the Tor network. Examples of hidden services websites are the aforementioned AlphaBay and Hansa. Tor is available on cellphones using the Android and Apple operating systems by installing an application that puts a TOR-enabled internet browser on a user's cellphone, which then routes the phone's IP address through different servers all over the world, making it extremely difficult to track.

[2] Fiat currency is currency created and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

d. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[3] Cryptocurrency is not illegal in the United States.

e. Bitcoin[4] ("BTC") is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other

[3] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

[4] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his/her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it's not completely anonymous, Bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems.

f. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key.") A public address is represented as a case-sensitive string of letters and numbers, 26–25 (35) characters long.

Each public address is controlled and/or accessed through the use of a unique corresponding private key - the cryptographic equivalent of a password or PIN - needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

g. Although cryptocurrencies such as Bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft-used means of payment for illegal goods and services on hidden services websites operating on the Tor network. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplaces. As of April 1, 2021, one bitcoin is worth approximately $59,000.00, though the value of bitcoin is generally much more volatile than that of fiat currencies.

h. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available

device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[5] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

i. Bitcoin "exchangers" and "exchanges" are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to the Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[6] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional

[5] A QR code is a matrix barcode that is a machine-readable optical label.

[6] *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," *available at* https://www.fincen.gov/resources/statutes-regulations/guiadance/application-fincens-regulations-persons-administering.

financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and/or the full bank account and routing numbers that the customer links to his/her exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who not only lack AML or KYC protocols but often advertise their ability to offer customers stealth and anonymity. These illicit exchangers often exchange fiat currency for cryptocurrencies, such as by meeting customers in person or by shipping fiat currency through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9-10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1-2%).

j. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet

application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), investigators may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

PROBABLE CAUSE STATEMENT

SUMMARY OF THE INVESTIGATION

20. On October 04, 2019 the SCHCTF in Columbus, Ohio, consisting of investigators assigned to HSI, Drug Enforcement Administration (DEA), United States Postal Inspection Service (USPIS) and the Internal Revenue Service (IRS), executed a federal search warrant at a Columbus Target's residence, who was using an online moniker to purchase narcotics off the Darknet site Empire Market. Investigators found and seized computers, mobile phones, media storage devices, $43,097.00 in U.S. currency, one 9mm pistol with a loaded magazine, controlled substances and miscellaneous documents from the residence. Analysis of the Columbus Target's mobile phone, along with his Darknet Empire Market account, indicated that he had been communicating with and purchasing liquid psychedelic mushrooms from an online vendor using the Darknet moniker "TRIPWITHSCIENCE" on a regular basis.

21. Open source research determined that "TRIPWITHSCIENCE" operated on several Darknet markets since approximately 2011, totaling over 17,000 transactions: Empire Market (4,719 transactions), Agora (1,500 transactions), Apollon Market (47 transactions), Berlusconi Market (60 transactions), Cryptonia Market (199 transactions), Dream Market (6,400 transactions), Tochka Market (542 transactions), Hansa Market (567 transactions), Silk Road 2.0 (2,199 transactions) and Dark Market (823 transactions). The

research also indicated that "TRIPWITHSCIENCE" may have operated on Nightmare Market, Andromeda Market, AlphaBay, Silk Road, Wall Street Market, Pandora, Black Market Reloaded, and numerous other small Darknet markets, but the number of transactions associated with those markets is unknown.

22. On April 21, 2021, BARLOW, the individual using the moniker "TRIPWITHSCIENCE", among others, on various darknet markets since approximately 2013, was arrested in Las Vegas, Nevada, pursuant to a federal criminal complaint issued by a Federal Magistrate Judge in the Southern District of Ohio. In the complaint, BARLOW was charged with federal narcotics violations to include Title 21, United States Code Sections § 841 and § 846, both statutes previously described in this affidavit.

23. Up to the date of his arrest, "TRIPWITHSCIENCE" was actively operating on Monopoly, Televend and Cannahome Darknet marketplaces selling liquid psychedelic mushrooms in 9.0 milligram/gram vials for $19.95 each. "TRIPWITHSCIENCE" specifically stated how to consume the controlled substance on his marketplace listings, verifying the controlled substance analogue is for human consumption.

24. From December 23, 2019 through November 20, 2020, HSI Columbus, with assistance from DEA and USPIS, conducted twelve (12) controlled liquid mushroom buys from "TRIPWITHSCIENCE" via Empire and Cannahome Markets. HSI Columbus purchased a total of approximately 545 grams of liquid psychedelic mushrooms during the twelve buys. HSI received and seized a U.S. Mail parcel associated with each buy containing suspected liquid psychedelic mushrooms. The Ohio Bureau of Criminal Investigation (BCI) Forensic Laboratory tested the contents of each parcel and determined them to be 4-Acetoxy-N,N-Dimethyltryptamine (4-AcO-DMT). This controlled substance is an analogue of 4-

Hydroxy-N,N-Dimethyltryptamine (liquid psychedelic mushrooms), a schedule I controlled substance.

25. On or about October 22, 2020, HSI Columbus received data from a seized Darknet Marketplace that contained 34 Bitcoin withdrawal wallet addresses for "TRIPWITHSCIENCE's" vender account. Using cryptocurrency analysis tracing, a Coinbase wallet was discovered sending and receiving Bitcoin from "TRIPWITHSCIENCE's" withdrawal wallets.

26. Investigators subpoenaed Coinbase for the subscriber information and the account history associated with the Coinbase customer conducting the bitcoin transactions. The Coinbase subpoena returns revealed the following:

- BARLOW's account was created on January 22, 2013, and was still open and active;
- BARLOW's account was a merchant account using the company name Royal Bowmen;
- BARLOW listed three bank accounts in which crypto-currency converted to fiat currency could be deposited by Coinbase. Those accounts were located at Ally Bank (accounts ending in #4088 and #4065 and in the name of BARLOW), Chase Bank (account ending in #8811 and in the name of Nutra HQ), and Wells Fargo (account ending in #6376 and in the name of BARLOW.)

27. Coinbase records showed that BARLOW sold approximately 312.99 Bitcoins through the exchange, which, at the time of the transaction was valued at $717,461.27, but only purchased 1 Bitcoin valued at $188.94 (at the time of transaction) during the same time frame. Similarly, BARLOW sold both 81.11 Ethers valued at $52,576.26 and 492.13

Litecoins valued at $30,828.25 but did not make any purchases for those cryptocurrencies on the exchange.

28. While reviewing seized Darknet Marketplace data from "TRIPWITHSCIENCE," HSI SAs discovered messages between "TRIPWITHSCIENCE and the Darknet moniker "DARKLOIS." The messages identified "DARKLOIS" as a shill[7] account created by "TRIPWITHSCIENCE" to promote his business and create test shipments on his account. Agents discovered a similar conversation between "DARKLOIS" and Darknet vendor "PERFECTSHROOMS," the only other account "DARKLOIS" reviewed and interacted with. HSI Agents identified two additional shill Darknet buyer accounts, "APPLETITS" and "BOTTLEWHISKEYSHL," being used by "TRIPWITHSCIENCE" and "PERFECTSHROOMS" to promote their sales on multiple Darknet marketplaces including Hansa Market.

29. Up until the date of his arrest, "PERFECTSHROOMS" had listings on Televend, Monopoly and Cannahome marketplaces. The account had listings for 3.5 grams to 114 grams of "Organic Mushrooms" (Psilocybe Cubensis Shrooms) in capsule form. A February 14, 2020, Established Vender Application states[8] PerfectShrooms has processed 7,800 orders on 15 different darknet marketplaces.

---

[7] A shill account is an account created to promote something or someone without divulging their association to the entity.

[8] Established Vendor Applications are used by vendors applying to a new marketplace. Vendors will list the markets they have sold on and how many transactions they've completed in an attempt to get discounted or waived vendor fees.

30. On or about January 4, 2021, HSI Columbus received electronic results from a search warrant issued to Google for records associated with Jim.V.Barlow@gmail.com. In the records were multiple spreadsheets referencing Darknet marketplaces and bitcoin transactions believed to be sales ledgers for "TRIPWITHSCIENCE" and "PERFECTSHROOMS." In a spreadsheet titled "2015 TCS Accounting" were 9 tabs, 7 of the tabs were titled 2015 and contained known two letter abbreviations for darknet markets AlphaBay, Nucleus Market, Abraxas Market, MiddleEarth Marketplace, Evolution Market, Agora Market and Black Bank Market. Each spreadsheet listed multiple transactions that included a date, time, a notation that payment was received, and a blockchain transaction hash. HSI Columbus analyzed several of the bitcoin blockchain transaction hashes using crypto currency analysis tools and results confirmed the transactions hash.

31. A tab titled "2015 Received" appeared to list all 704 Darknet transactions from January 1, 2015 through December 9, 2015. Per the spreadsheet, these 704 Darknet transactions netted approximately 1,544.984636 bitcoins equaling $401,816.78 in 2015. Due to the steady rise of bitcoin's value, those 1,544.984636 bitcoins are worth approximately $86,028,298.00 (as of March 29, 2021).

32. An investigative search conducted on the darknet website Empire Market for the vendor "TRIPWITHSCIENCE" revealed a listing for "Liquid Mushrooms (Pure Psilocybin Extract)." The listing advertised vials of approximately 9mg of "Liquid Mushrooms" for $19.95 each. The listing allowed buyers to purchase in unlimited quantities/increments. This search revealed "TRIPWITHSCIENCE," who was active on the market from December 3, 2018 through November 23, 2019, had completed 2,555 transactions. There were 1,732 positive feedback comments left for "TRIPWITHSCIENCE" during that time frame, which

regularly commented on the quality of the product. The feedback represented drug transactions ranging from $27.90 and $2,004.85. Investigators determined that these 2,555 transactions (valued between $27.90 and $2,004.85 per transaction) generated between $71,000 and $5,110,000 in proceeds.

33. On December 2, 2018, one bitcoin was valued at approximately $3,300, by June 2019, one bitcoin's value rose to approximately $13,000. Depending on the date of transaction, this equates to an increase in bitcoin value of approximately 450% to 1,700%. Total value of "TRIPWITHSCIENCE's" drug transactions conducted on the darknet website Empire Market between December 3, 2018 and November 23, 2019, are currently estimated to be worth approximately $320,000 to $90,855,000.

34. While reviewing the results from Google of BARLOW's Gmail account, investigators found a second spreadsheet titled "TCS Accounting." In the spreadsheet were tabs for each year from 2014 to 2021 and a summary tab. Each tab, dated for a certain year, showed a detail ledger. Many of the ledgers included references to Darknet marketplaces, bitcoin mixing services and drug transactions. The summary tab broke down each year's net, average month, average day, and total bitcoins earned for the year. The summary page noted that James BARLOW earned 2,299.49539 bitcoins from 2014 through 2020. Investigators know that these 2,299.49539 bitcoins are currently worth approximately $77,968,990.20.

35. A third spreadsheet titled "TWS Sales Summation" was found by investigators on BARLOW's Google Drive in a folder named "DNM," known by law enforcement to be an abbreviation for Darknet Market. The spreadsheet showed a sales ledger for Liquid Mushrooms sold in July of 2014 on Silk Road, Agora and Evolution Darknet markets. The ledger claimed, at the time, BARLOW was averaging 682 orders a month and selling

approximately 2,555 vials per month. At $19.95 per vial, BARLOW was averaging $50,972.25 a month in drug proceeds on the three Darknet marketplaces. In July of 2014, bitcoin's average value was approximately $635 per bitcoin. Your affiant divided $635 by BARLOW's average monthly sales of $50,972.25 to determine that BARLOW was making approximately 80 bitcoin per month in July of 2014. If unspent, the 80 bitcoin BARLOW was making per month since July of 2014 would currently be valued at approximately $4,710,040.

36. Additional results from BARLOW's Google Drive account confirmed BARLOW was darknet vendor "TRIPWITHSCIENCE." BARLOW owned or co-owned several business including Nutra HQ, Vegas Views, Good-To-Glow, Illuminated Couture and Royal Bowman. The evidence gathered and analyzed by investigators related to these businesses revealed that BARLOW was not generating enough, if any, income from these businesses to support his lifestyle, which included travel on private jets, world travel, purchases of high-end automobiles, and ownership of multiple properties, including a $1.5 million property purchased by BARLOW in March 2021.

37. Investigators believe BARLOW's only known employment was with the United States Army where he was an E7 earning approximately $4,000 a month. BARLOW is believed to have retired from the Army in 2020. Prior to his arrest, BARLOW was living in Las Vegas in a rented house with two roommates. BARLOW co-owned a second residence with one of his roommates that they rented out on Airbnb. BARLOW owns two Tesla cars, two jet skis and a dodge van. BARLOW purchased at least two other Tesla cars for his friends in prior years.

LAUNDERING OF NARCOTICS PROCEEDS

38. Transactions on DWMs such as those described in this affidavit are conducted through the use of cryptocurrency, primarily Bitcoin, in order to facilitate anonymity. Proceeds from transactions on DWMs are deposited to a common wallet within the DWM known as a "hot wallet," and available balances are tracked within each user account. When a vendor wants to withdraw funds from the DWM, he/she withdraws Bitcoin from his/her DWM "account" to a Bitcoin address within his/her control. Bitcoin from the hot wallet is then transferred to the address indicated by the vendor. These financial transactions, conducted with the proceeds of illegal narcotics sales, were executed with the knowledge that it would conceal the nature, source, and origin, of such proceeds, constituting money laundering transactions under Title 18 U.S.C. § 1956.

39. To obtain fiat value from cryptocurrency, it must be exchanged from Bitcoin to the individual's fiat currency of choice (e.g., USD, GBP, or some denomination). This transformation of value occurs at cryptocurrency exchanges, such as Coinbase, Binance, Kraken, or other like exchanges, which are money services businesses (MSBs). In order to use an exchange, an individual must create an account at the exchange and then send Bitcoin, or other form of cryptocurrency, from an address they control to an address associated with their account at the cryptocurrency exchange. The individual could then withdraw funds from the cryptocurrency exchange to their bank of choice; alternately, it could be exchanged for other forms of cryptocurrency (e.g., Ethereum, Litecoin, etc.). Conducting financial transactions with the proceeds of illegal narcotics sales with the knowledge that it would conceal their nature, source, and origin, e.g., converting pseudonymous bitcoin proceeds into seemingly legitimate fiat currency, constitutes money laundering under 18 U.S.C. § 1956.

40. Because of the nature of how bitcoin is transferred between addresses, tracing a bitcoin transaction is akin to tracking a serialized dollar through the financial system. As a result, it is impractical to employ traditional tracing methods to complex, multi-hop bitcoin transactions. Instead, bitcoin flow analysis shows the overall path of where bitcoin came from prior to reaching a certain wallet or address. So, while the activity may not be directly traceable at the transactional level, it can often be indirectly traced back to an origin wallet or address. Because every bitcoin transaction is entered into the public blockchain ledger, investigators can use historical blockchain analysis to determine which origin wallets belong to bitcoin addresses well-known to law enforcement, such as DWMs (e.g., Silk Road 1, Hansa, etc.), exchanges (e.g., Coinbase, Binance, Kraken, etc.), or peer-to-peer exchange platforms (e.g., LocalBitcoins). Wallets and addresses that belong to unknown individuals, however, are far more difficult to identify.

41. Using historical blockchain analysis, bitcoin flow analysis, and the information received from the issuance of legal process, law enforcement was able to determine the following:

a. funds deposited into accounts at Coinbase, Binance, Celsius, and other regulated exchanges represent an attempt, by BARLOW, to cash out the proceeds of crime, specifically proceeds derived from the sale of narcotics via several darknet markets;

b. In addition to the direct tracing of criminal proceeds from the Hansa market, blockchain analysis suggests BARLOW's accounts at Coinbase, Binance, Circle, Gemini, and others, indirectly received between 4% and 13% of funds from addresses allegedly controlled by darknet markets or vendors;

c. BARLOW's accounts at these same exchanges, and wallet clusters suspected of being owned and controlled by BARLOW, indirectly and directly have received between 40% and 70% of funds from mixing services[9] such as WasabiWallet, SharedCoin, BestMixer, BitMixer, and HelixMixer. Further, identified co-conspirators of BARLOW have been paid directly from these same mixing services in exchange for assisting BARLOW with trafficking in drugs;

d. Some of BARLOW's self-hosted wallets appear to have received nearly all funds from mixers like WasabiWallet.

ASSETS SUBJECT TO FORFEITURE

BARLOW's WEALTHFRONT BROKERAGE ACCOUNT

42. Records obtained from Wealthfront Brokerage ("Wealthfront"), LLC, revealed that, on, or about, February 23, 2016, BARLOW opened his WFB#5396 investment account. Your affiant reviewed/analyzed the records provided by Wealthfront for the time period beginning when the account opened through March 31, 2021. The following is summary of the pertinent information:

a. During the period analyzed, there was approximately $582,612 deposited into BARLOW's WFB#5396 account. A majority (approximately 79%) of the deposits made into this account were funds from two different bank accounts owned by BARLOW. These accounts were held at Wells Fargo and Ally Bank.

[9] Mixing services are known to law enforcement to be used by criminal organizations to obfuscate the transfer of criminal proceeds. High-risk exchanges operating in jurisdictions with little to no regulation, Know-Your-Customer (KYC) or Anti-Money Laundering (AML) requirements, are known to law enforcement to be used by criminal organizations to launder or cash out criminal proceeds generated through the sale of narcotics and other illicit goods on the dark web.

b. Approximately $152,600 of the deposits made into this account were from the repayment of loans taken from the brokerage account by BARLOW. On at least 4 occasions BARLOW borrowed funds from the WFB#5396. On each occasion, BARLOW repaid those loans to his own brokerage account within 90-120 days.

c. The last deposit made into the WFB#5396 was made on March 16, 2021, a little over one month prior to BARLOW's arrest. The deposit was in the amount of $60,000 and came from BARLOW's Ally Bank account.

43. Investigators obtained and analyzed the records related to the two bank accounts that funded the seventy-nine percent of BARLOW's WFB#5396 account. The following is a summary of the pertinent and/or relevant information related to each of these accounts:

BARLOW's Wells Fargo account

a. On or about, August 11, 2016, a checking account, ending in #6376 (previously referenced in this affidavit) was opened in BARLOW's name at Wells Fargo Bank (hereinafter referred to as WELLS#6376). Analysis of the bank records revealed that between January 1, 2017 and February 19, 2021, there was approximately $500,007 deposited into this account. Approximately $452,887 of the deposits were from the following:

- Approximately $214,887 from BARLOW's, or one his associates, Coinbase account, previously referenced in this affidavit;
- Approximately $117,00 in cash; and
- Approximately $121,000 in loans from BARLOW's WFB#5396 account.

b. During this same period of time, bank records revealed that approximately $225,718 was sent from BARLOW's WELLS#6376 account to BARLOW's

WFB#5396 account. In most, if not all, occasions, a deposit from BARLOW's, or one of his associates, Coinbase accounts was made into the WELLS#6376 within days preceding the outgoing disbursements to BARLOW's WFB#5396 account. An example of such transactions are as follows:

Transaction Date	Deposit Amount	Withdrawal Amount	Source of Deposit	Payee
01/09/2019	$23,114.00		Coinbase	
01/28/2019	$20,000.00		Coinbase	
01/29/2019		$23,000.00		Wealthfront, Inc.
01/29/2019		$20,000.00		Wealthfront, Inc.
02/25/2019	$2,000.00		Coinbase	
03/13/2019	$13,000.00		Coinbase	
03/19/2019		$14,570.00		Wealthfront, Inc.
10/30/2020	$8,583.17		Coinbase	
10/19/2020		$8,593.17		Wealthfront, Inc.
01/05/2021	$10,701.25		Coinbase	
01/08/2021	$11,700.77		Coinbase	
01/11/2021		$10,701.25		Wealthfront, Inc.
01/14/2021		$11,700.77		Wealthfront, Inc.

BARLOW's Ally Bank account

c. On or about, March 31, 2010, a checking account, ending in #4065 was opened in BARLOW's name at Ally Bank (hereinafter referred to as AB#4065). Analysis of this account revealed that between January 3, 2017, and April 25, 2021, there was approximately $1,829,924 deposited into this account. Approximately $1,695,150 of the deposits were from a BARLOW, or one of his associates, owned Coinbase account.

d. During this same period of time, bank records show that approximately $233,894 was sent from BARLOW's AB#4065 account to BARLOW's WFB#5396. In

most, if not all, occasions, a deposit from BARLOW's, or one of his associates, Coinbase account(s) was made into the WELLS#6376 account within days preceding the outgoing disbursements to BARLOW's WFB#5396 account. An example of such activity is as follows:

Transaction Date	Deposit Amount	Withdrawal Amount	Source of Deposit	Payee
12/11/2017	$29,103.31		Coinbase	
12/19/2017		$25,000.00		Wealthfront, Inc.
09/24/2018	$11,875.32		Coinbase	
09/24/2018	$13,280.42		Coinbase	
09/25/2018		$25,000.00		Wealthfront, Inc.
10/11/2019	$8,416.85		Coinbase	
10/17/2019		$5,000.00		Wealthfront, Inc.
01/21/2020	$12,733.15		Coinbase	
01/22/2020		$10,000.00		Wealthfront, Inc.

44. As previously noted, funds from BARLOW's Wells Fargo and Ally Bank accounts funded seventy-nine percent of the contributions into BARLOW's WFB#5396. A large portion of the contributions were made following a deposit of funds from BARLOW's, or one of his associates, Coinbase account(s) into his accounts at Wells Fargo and Ally Bank. As previously stated in this affidavit, blockchain analysis suggests that BARLOW's accounts at Coinbase, Binance, Circle, and Gemini, indirectly received between 4% and 13% of funds from addresses allegedly controlled by darknet markets or vendors. BARLOW's accounts at these same exchanges, and wallet clusters suspected of being owned and controlled by BARLOW, indirectly and directly have received between 40% and 70% of funds from mixing services such as WasabiWallet, SharedCoin, BestMixer, BitMixer, and HelixMixer, which are most commonly used to obfuscate the true nature, origin, or source, of such funds.

BARLOW's TESLA (MODEL X)

45. Records obtained from Tesla, Inc., revealed that on, or about, December 27, 2016, BARLOW purchased a 2016 TESLA, Model X P100D, VIN #5YJXCDE45GF026419 (hereinafter referred to as 'Subject Tesla') from Tesla Motors NV, Inc., for approximately $170,282. Tesla records revealed that BARLOW purchased this vehicle with funds from the following:

a. A loan, in the amount of $50,000, from USAA Federal Savings.

b. a $5,000 payment via PayPal.

c. a cashier's check, in the amount of $5,312.73 purchased by BARLOW from Bank of America (BOA).

d. a cashier's check, in the amount of $109,998, purchased by BARLOW from Wells Fargo Bank.

46. Information provided by USAA revealed that on, or about, February 1, 2017, BARLOW obtained a loan in the amount of $50,000 towards the payment/purchase of the Subject Tesla. Per the USAA loan application, BARLOW was self-employed in the "Health Supplements" industry, with an annual income of $250,000 per year. This loan was funded (funds sent to Tesla, Inc.) by USAA on, or about, February 1, 2017. The loan was paid off, via several payments, on, or about, February 28, 2017, just four weeks after it was funded.

47. Records obtained from BOA and analyzed by investigators revealed that on, or about, August 13, 2016, a checking account, ending in #7110, was opened in BARLOW's name (hereinafter referred to as BOA#7110). Per the records obtained, the BOA cashier's check, in the amount of $5,312.73 and used towards the purchase of the Subject Tesla, was purchased with funds withdrawn from BARLOW's BOA#7110 account.

48. Records obtained from Wells Fargo Bank and analyzed by your affiant revealed that the cashier's check, in the amount of $109,998.70 and used towards the purchase of the Subject Tesla, was purchased with funds withdrawn from two different bank accounts, both belonging to BARLOW. The first withdrawal, in the amount of $27,271.67, was made from BARLOW's WELLS#6376 account previously referenced in this affidavit. The second withdrawal, in the amount of $82,737.03, was made from Wells Fargo bank savings account, ending in #5780, also in the name BARLOW (hereinafter referred to as WELLS#5780). Per Wells Fargo records, BARLOW's WELLS#5780 account was opened on August 11, 2016.

49. In BARLOW's Google drive, analyzed by investigators and previously referenced in this affidavit, investigators observed a video titled "IMG_6950"-"IMG_6960" which appeared to be taken on February 12, 2021. The video was of BARLOW explaining how he purchased land in Colorado using Bitcoin. BARLOW further explained that he took out a loan using Bitcoin as collateral and that in 2016 he bought a Tesla for $170,000 after liquidating 286 Bitcoin. On July 16, 2021, a federal law enforcement officer observed BARLOW's 2016 Tesla, Model X, parked in the driveway of BARLOW's residence at 1409 Bonita Avenue, Las Vegas, Nevada, 89104.

50. Very few, if any, of the products/services being sold on DWMs are legal (e.g., contraband such as heroin) or are being sold legally (e.g., illegal sales of prescription drugs). Therefore, bitcoins being withdrawn from the DWM's represents proceeds of illegal activity in nearly every instance. Because the bitcoins being withdrawn from the DWM's consist almost entirely of criminal proceeds, I submit there is probable cause to seize the SUBJECT ASSETS belonging to BARLOW.

51. On May 18, 2021, BARLOW, along with several others, were indicted by a federal grand jury in the Southern District of Ohio (United States v James V. Barlow, et al. SDOH Case No. 2:21-cr-089), with Conspiracy to Possess with Intent to Distribute Psychedelic Mushroom Analogue, in violation of 21 U.S.C. §§ 841(a)(1) and (b)(1)(C) and 21 U.S.C. §846. The Indictment also notified BARLOW that, in accordance with 21 U.S.C. § 853, the United States intends to seek the forfeiture of all property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of the violations alleged in the Indictment, and any property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of such violations, including, but not limited to, the SUBJECT ASSETS.

52. Therefore, I respectfully request the issuance of Federal Search and Seizure Warrants for the 2016 Model X, a passenger vehicle, with a Vehicle Identification Number (VIN) 5YJXCDE45GF026419, including all keys and any and all ownership and/or registration documents for said vehicle, and all funds and/or digital currencies held in Wealthfront Brokerage account #8W285396, held in the name of James BARLOW.

Stephen M Blunk

SPECIAL AGENT STEPHEN BLUNK
Internal Revenue Service, Criminal Investigation

Sworn to and subscribed before me on
this 2nd day of ~~July~~ AUGUST 2021.

Elizabeth A. Preston Deavers

THE HONORABLE ELIZABETH A. PRESTON DEAVERS
UNITED STATES MAGISTRATE JUDGE